Avaya 3100 Mobile Communicator

Troubleshooting

Release: 3.1
Document Revision: 02.03

NN42030-700

Avaya 3100 Mobile Communicator
Release: 3.1
Publication: NN42030-700
Document release date: 15 July 2010

© 2008-2010 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support

Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright

Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

New in this release 7
Features 7
Other changes 7

Overview 9
References 9

Accessing the system 11
Logging on to the Avaya 3100 Mobile Communicator Web Console as an administrator 11
Logging on to the Avaya 3100 Mobile Communicator Web Console as an administrator 11
Changing the Avaya 3100 Mobile Communicator Web Console password 13
Resetting the Web Administration Console administrator password 14
Accessing the server command line as nortel 15
Accessing the server command line as superuser 15

Troubleshooting unresponsive systems 17

Troubleshooting and maintenance of Avaya 3100 Mobile Communicator 19
Troubleshooting license file problems 19
Using log files 20
Downloading all log files 21
Downloading an individual log file 22
Sorting the log files 22
Opening a log file 23

Troubleshooting communication and network problems 25
Performing a packet capture 25
Disabling Wireshark packet checksum verification 26

Troubleshooting data connections between Avaya 3100 Mobile Communicator - Client for Windows Mobile and the gateway 29

Troubleshooting client log in problems 31
Log in problem scenario setup 32
Client log in problem analysis 34

Troubleshooting call termination problems 37
Call termination problem scenario setup 38
Call termination problem analysis 40

Troubleshooting call origination problems 43
Call origination problem scenario setup 44
Call origination problem analysis 46

Troubleshooting corporate directory search problems 51
Corporate directory search problem scenario setup 52
Corporate directory search problem analysis 54

New in this release

The following sections details what's new in *Avaya 3100 Mobile Communicator Troubleshooting* (NN42030-700) for Avaya 3100 Mobile Communicator Release 3.1.

- "Features" (page 7)
- "Other changes" (page 7)

Features

For information about all the Avaya 3100 Mobile Communicator Release 3.1 features, see *Avaya 3100 Mobile Communicator Fundamentals* (NN42030-109).

Other changes

The following changes were made for Avaya 3100 Mobile Communicator Release 3.1:

- Updated the list of referenced books
- Retitled *System recovery* chapter to *Troubleshooting unresponsive systems*.
- Renamed Web Console to Web Administration Console

Revision history

July 2010	Standard 02.03. This document is issued to support Avaya 3100 Mobile Communicator Release 3.1. This document contains editorial changes.
November 2009	Standard 02.02. This document is issued to support Avaya 3100 Mobile Communicator Release 3.1. Information was updated in "Changing the Avaya 3100 Mobile Communicator Web Console password" (page 13) and "Performing a packet capture" (page 25). "Resetting the Web Administration Console administrator password" (page 14) was added.
October 2009	Standard 02.01. This document is issued to support Avaya 3100 Mobile Communicator Release 3.1.

June 2009	Standard 01.03. This document is issued to support Avaya 3100 Mobile Communicator Release 3.0 SU3. Changes were made to technical content.
January 2009	Standard 01.02. This document is issued to support Avaya 3100 Mobile Communicator Release 3.0. Changes were made to "Downloading all log files" (page 21), "Downloading an individual log file" (page 22), "Sorting the log files" (page 22), and "Performing a packet capture" (page 25).
September 2008	Standard 01.01. This document is issued to support Avaya 3100 Mobile Communicator Release 3.0.

Overview

This document provides information about the troubleshooting of the Avaya 3100 Mobile Communicator.

Navigation

- "Accessing the system" (page 11)
- "Troubleshooting unresponsive systems" (page 17)
- "Troubleshooting and maintenance of Avaya 3100 Mobile Communicator" (page 19)
- "Troubleshooting communication and network problems" (page 25)
- "Troubleshooting data connections between Avaya 3100 Mobile Communicator - Client for Windows Mobile and the gateway" (page 29)
- "Troubleshooting client log in problems" (page 31)
- "Troubleshooting call termination problems" (page 37)
- "Troubleshooting call origination problems" (page 43)
- "Troubleshooting corporate directory search problems" (page 51)

References

For more information, see the following documents:

- *Avaya 3100 Mobile Communicator Fundamentals* (NN42030-109)
- *Avaya 3100 Mobile Communicator for BlackBerry User Guide* (NN42030-101)
- *Avaya 3100 Mobile Communicator for Nokia User Guide* (NN42030-102)
- *Avaya 3100 Mobile Communicator for Windows Mobile User Guide* (NN42030-107)
- *Avaya 3100 Mobile Communicator for iPhone User Guide* (NN42030-111)
- *Avaya 3100 Mobile Communicator Web User Interface User Guide* (NN42030-110)

- *Avaya 3100 Mobile Communicator Administration and Security* (NN42030-600)
- *Avaya Deployment Guide* (NN42040-301)

Accessing the system

This module provides information about the ways to access the system from the Web Administration Console and from the command line.

Navigation

- "Logging on to the Avaya 3100 Mobile Communicator Web Console as an administrator" (page 11)
- "Changing the Avaya 3100 Mobile Communicator Web Console password" (page 13)
- "Resetting the Web Administration Console administrator password" (page 14)
- "Accessing the server command line as nortel" (page 15)
- "Accessing the server command line as superuser" (page 15)

Logging on to the Avaya 3100 Mobile Communicator Web Console as an administrator

This module describes the procedure you use to log on to Avaya 3100 Mobile Communicator Web Console to perform administration tasks.

Logging on to the Avaya 3100 Mobile Communicator Web Console as an administrator

Log on to the Avaya 3100 Mobile Communicator Web Console as an administrator to manage the system, monitor the users, monitor Instant Conferencing, and manage the client server repository.

Attention: Wait two minutes after starting the Avaya 3100 Mobile Communicator Gateway before accessing the Avaya 3100 Mobile Communicator Web Console.

Prerequisites

- You need the administrator user id and password to perform this procedure.
- Access the Avaya 3100 Mobile Communicator Web Console using a web browser.

Attention: User names and passwords are case-sensitive.

Procedure steps

Step	Action
1	In the **Address** field of your Web browser, enter **`http://<IP address	hostname>:8282/adminserver`** **OR** **`https://<IP address	hostname>:8553/adminserver`**
2	In the **Username** field, type the user name.
3	In the **Password** field, type the admin password. **Attention:** Avaya recommends that you change the default administrator password. For more information, see "Changing the Avaya 3100 Mobile Communicator Web Console password" (page 13).
4	Click **Sign In**.
5	Click a tab at the top of the Avaya 3100 Mobile Communicator Web Console to view the corresponding page.

--End--

Variable definitions

Variable	Value
<IP address | hostname>	The name of the Avaya 3100 Mobile Communicator Gateway server in fully qualified domain name (FQDN) format, or the IP address of the server.

Variable	Value
user name	Default: admin
admin password	Default: password

Changing the Avaya 3100 Mobile Communicator Web Console password

Change the Avaya 3100 Mobile Communicator Web Console password from the default password.

Prerequisites

- You must be logged into the Avaya 3100 Mobile Communicator Web Console as administrator. For more information, see "Logging on to the Avaya 3100 Mobile Communicator Web Console as an administrator" (page 11).

Procedure steps

Step	Action
1	On the Avaya 3100 Mobile Communicator Web Console main page, click the **Tools** tab.
2	In the **Admin Server Password** section, in the **Current Password** box, type the current password.
	Attention: Passwords are case-sensitive.
3	In the **New Password** box, type a new password.
4	In the **Confirm New Password** box, retype the new password.
5	In the **Admin Server Password** section, click **Save**.
	--End--

Variable definitions

Variable	Value
Current Password	Existing password. The default password for new servers is *password*

Variable	Value
New password	New password for the Admin server. Secure passwords use a mix of letters, numbers and alphabetic characters and can be up to 19 characters in length.
Confirm New Password	New password for confirmation.

Resetting the Web Administration Console administrator password

Use this procedure to reset the Avaya 3100 Mobile Communicator Web Administration Console administrator password.

Prerequisites

- You must be logged in to the server as nortel. For more information, see "Accessing the server command line as nortel" (page 15).

Procedure steps

Step	Action
1	Enter the following command: **su -** If prompted, enter the root password.
2	Enter the following command: **/opt/MobilityGateway/etc/resetadminpw.sh** The tool changes the administrator password to `password`

Attention: Avaya recommends that you immediately change the password to a more secure password.

--End--

Accessing the server command line as nortel

Use this procedure to access the server command line as nortel.

Prerequisites

- You require the password to the nortel userid on the server.

Procedure steps

Step	Action
1	Use SSH to connect to the server.
2	At the userid prompt, enter **nortel**
3	At the password prompt, enter <password>

--End--

Variable definitions

Variable	Value
<password>	The password associated with the nortel userid. For information about the default nortel password, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Accessing the server command line as superuser

Use this procedure to access the server command line as root.

Prerequisites

- You require the password to the nortel userid on the server.
- You require the password to the superuser (root) userid on the server.

Procedure steps

Step	Action
1	Use SSH to connect to the server.
2	At the userid prompt, enter **nortel**
3	At the password prompt, enter <password>
4	To become the root user, enter **su root**
5	At the prompt, enter <root_password>

--End--

Variable definitions

Variable	Value
<password>	The password associated with the nortel userid. For information about the default nortel password, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).
<root_password>	The password associated with the superuser. For information about the default superuser password, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Troubleshooting unresponsive systems

This chapter describes the actions you take if your system becomes unresponsive.

1. Work through the troubleshooting procedures in the next sections of this book.
2. If your system is still unresponsive, execute "Downloading all log files" (page 21).
3. Save the log files on another computer in preparation for assistance from Avaya.
4. Access the command line, using "Accessing the server command line as nortel" (page 15).
5. Enter the following command:
   `ps`
6. Record the information displayed on the screen.
7. Contact your Avaya support organization immediately.

Attention: Do not reboot or restart your system. The Avaya technical support team may require additional information.

---

8. The Avaya support organization will instruct you on to the next steps to take.

Troubleshooting and maintenance of Avaya 3100 Mobile Communicator

The following modules describe the Avaya 3100 Mobile Communicator troubleshooting and maintenance.

- "Troubleshooting license file problems" (page 19)
- "Using log files" (page 20)

Troubleshooting license file problems

If you encounter a problem with the license file installation, an error message appears in the License Info field on the System Configuration window. The following table lists the most common error messages and possible solutions.

Table 1
License file error messages

Error message	Description	Solution
License Info: License file not found	The Avaya 3100 Mobile Communicator Gateway is not activated and requires the license file.	Upload the license file on the System Configuration screen.
License Info: License is invalid	The Avaya 3100 Mobile Communicator Gateway is using another activated machine's license file.	Upload a valid license file on the System Configuration screen.
License Info: License expired	The license file is no longer valid.	Upload a valid license file on the System Configuration screen.

Table 1
License file error messages (cont'd.)

Error message	Description	Solution
License Info: ERROR 23: protocol violation	The Avaya 3100 Mobile Communicator Gateway is not activated although the license file is valid. The local system clock is out of sync with the licensing server clock.	Reset the clock and restart the system.
License Info: ERROR 103: Client's system clock is suspect and / or the client configur ation has been tampered with.	The system clock changed after the Avaya 3100 Mobile Communicator Gateway was activated.	Reset the clock and restart the system.
License Info: ERROR 17: key limit exceeded	The license file has been activated before with other machines and there are no licenses available for you to activate.	Contact the licensing server administrator.

If the recommended solution fails to correct the problem, or if the problem is not listed, contact the administrator of the licensing server for assistance.

Before contacting the administrator:

- Ensure that the date, time, and time zone for the system is synchronized with the licensing server.
- Check the network connection between your system and the licensing server (route, DNS).
- Check the most recent error message on the Gateway Configuration screen.
- Restart the server.

Using log files

The Avaya 3100 Mobile Communicator Gateway automatically generates the following log files:

- Boot log
- Avaya 3100 Mobile Communicator Gateway Alarms log

- Avaya Gateway log
- Server log
- Error log

The log files are generated on a daily basis, with the current day's output overwriting the output from preceding day.

Use the following procedures to handle the log files:

- "Downloading all log files" (page 21)
- "Downloading an individual log file" (page 22)
- "Sorting the log files" (page 22)
- "Opening a log file" (page 23)

Downloading all log files

You can download all the log files from the Avaya 3100 Mobile Communicator Gateway to a folder on your PC for analysis.

Prerequisites

- You must be logged into the Avaya 3100 Mobile Communicator Web Administration Console as administrator. For more information, see "Logging on to the Avaya 3100 Mobile Communicator Web Console as an administrator" (page 11).

Procedure steps

Step	Action
1	Click the **Tools** tab.
	The Tools page displays.
2	Scroll to the Server Logs section.
3	In the redundant configuration, select a gateway.
4	Click **Download all Logs**.
5	Click **Save**.
6	Navigate to the folder where you want to save the log files.
7	Click **Save**.
	The log files are saved.

--End--

Downloading an individual log file

You can download a single log file from the Avaya 3100 Mobile Communicator Gateway to a folder on your PC for analysis.

Prerequisites

- You must be logged into the Avaya 3100 Mobile Communicator Web Administration Console as administrator. For more information, see "Logging on to the Avaya 3100 Mobile Communicator Web Console as an administrator" (page 11).

Procedure steps

Step	Action
1	Click the **Tools** tab. The Tools page displays.
2	Scroll to the Server Logs section.
3	In the redundant configuration, select a gateway.
4	Click the **Download** link for the log file you wish to download: • boot.log • MobilityGateway-Alarms.log • MobilityGateway.log • server.log • sipconferror.log
5	Click **File, Save As**.
6	Navigate to the folder where you want to save the log file.
7	Click **Save**. The log file is saved.

--End--

Sorting the log files

You can sort the logs by name, file size, or date modified.

Prerequisites

- You must be logged into the Avaya 3100 Mobile Communicator Web Administration Console as administrator. For more information, see "Logging on to the Avaya 3100 Mobile Communicator Web Console as an administrator" (page 11).

Procedure steps

Step	Action
1	Click the **Tools** tab. The Tools page displays.
2	Scroll to the Server Logs section.
3	In the redundant configuration, select a gateway.
4	Click the column heading to sort the logs: • **Filename**—Sort in alphabetical order. • **Size (MB)**—Sort by file size. • **Last modified**—Sort by date modified.
5	To reverse the sorting order, click the column heading again.

--End--

Opening a log file

You can open the log files in a number of applications, including Hilios Text Pad, and Microsoft WordPad. Do not use the Microsoft default viewer (Notepad) because the log file does not display in an easily readable format.

Procedure steps

Step	Action
1	Browse to the folder where you have downloaded the log file.
2	Right-click the file, select **Open With, Choose Program**.
3	Select a file viewer application from the list. For example, WordPad.
4	Click **OK**. Open the log file in the file viewer application you selected.

--End--

Troubleshooting communication and network problems

The following modules describe the Avaya 3100 Mobile Communicator communication and network problem troubleshooting.

Navigation

- "Performing a packet capture" (page 25)
- "Disabling Wireshark packet checksum verification" (page 26)

Performing a packet capture

You can use the packet dump utility to capture all of the data transmitted and received on an interface of the Avaya 3100 Mobile Communicator Gateway for a period of time (a capture session). After the capture session completes, you can save the packet dump as a *.cap* file.

Attention: Before performing a packet capture, confirm that the server contains *tcpdump*. If necessary, install *tcpdump* in */usr/sbin*, and change the permissions by logging on as root and using the command **`chmod u+s /usr/sbin/tcpdump`**

To open the *.cap* files for troubleshooting and analysis, you require the protocol analyzer called Wireshark (formerly Ethereal).

Prerequisites

- You must be logged into the Avaya 3100 Mobile Communicator Web Administration Console as administrator. For more information, see "Logging on to the Avaya 3100 Mobile Communicator Web Console as an administrator" (page 11).

Procedure steps

Step	Action
1	Click the **Tools** tab.
2	Scroll to the Packet Capture section.
3	In the redundant configuration, select a gateway.
4	Click **Capture**.
5	Wait for the packet capture to be performed, then click **Stop**.
6	Click **Save**.
7	Navigate to the folder where you want to save the ***dump.cap*** log file.
8	Click **Save**. The ***dump.cap*** log file is saved.

--End--

Disabling Wireshark packet checksum verification

You need to disable Wireshark packet checksum verification before you can work with the captured packets.

Attention: When you view the packet captures from the Avaya 3100 Mobile Communicator Gateway packet capture utility, the trace contains incorrect checksums. The incorrect checksums occur because the network interface on the Avaya 3100 Mobile Communicator Gateway performs checksum off-loading, meaning that the network interface adds the checksum to the packets instead of the operating system TCP/IP stack. During the capture process, the host operating system sends the packets (being captured) directly to the capture interface without the addition of a checksum.

Wireshark performs checksum verification. Packet checksum errors can prevent TCP reassembly so you need to disable Wireshark checksum verification.

The following procedure provides the steps for Wireshark Version 0.99.6a (SVN Rev 22276). For more information, see the Wireshark documentation for your version of Wireshark or visit www.wireshark.org

Procedure steps

Step	Action
1	From the Wireshark **Edit** menu, select **Preferences**.
2	In the left pane of the **Preferences** dialog box, expand **Protocols**.
3	In the left pane of the **Preferences** dialog box, select **TCP** and clear the **Validate the TCP checksum if possible** check box.
4	In the left pane of the **Preferences** dialog box, select **UDP** and clear the **Validate the UDP checksum if possible** check box.
5	Click **Apply**.
6	Click **OK**.

--End--

Troubleshooting data connections between Avaya 3100 Mobile Communicator - Client for Windows Mobile and the gateway

Use this procedure to identify where problems originate when experiencing data connection problems between Avaya 3100 Mobile Communicator Gateway and Avaya 3100 Mobile Communicator - Client for Windows Mobile.

Procedure steps

Step	Action
1	Ping the Avaya 3100 Mobile Communicator Gateway from a PC to verify data connectivity of the PC to the Avaya 3100 Mobile Communicator Gateway.
2	If you cannot ping the Avaya 3100 Mobile Communicator Gateway, check the status of the Avaya 3100 Mobile Communicator Gateway.
3	Connect the mobile device to the computer with a USB cable.
4	Start Microsoft ActiveSync on the computer.
5	On the mobile device, select **Start, Internet Explorer**.
6	Browse to the Over the air download webpage to verify that the device can contact the Avaya 3100 Mobile Communicator Gateway Web Server. Depending on the type of security implemented on your system, enter one of the following: **http://<IP Address or FQDN of 3100 MCG>:8080/m** **OR** **https://<IP Address or FQDN of 3100 MCG>:8443/m**
7	If the Over the air download page can be accessed, then you have a data connection.

8	If the Over the air download page cannot be accessed, try accessing www.avaya.com.
9	If you can access the Avaya web site, but cannot access the Over the air download site, check the status of the network supporting the connection between the Avaya 3100 Mobile Communicator Gateway to Avaya 3100 Mobile Communicator - Client.
10	If you cannot access any web site, see your Windows Mobile support documentation to restore basic web browsing capability.

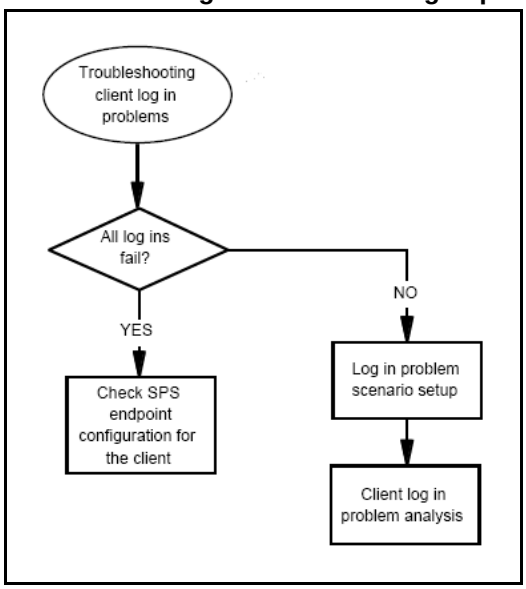
--End--

Troubleshooting client log in problems

Use this section to troubleshoot problems with client log ins.

Figure 1 "Troubleshooting tree for client log in problems " (page 31) shows the troubleshooting tree for this problem.

Figure 1
Troubleshooting tree for client log in problems


Troubleshooting client log in problems
All log ins fail?
NO
YES
Check SPS endpoint configuration for the client
Log in problem scenario setup
Client log in problem analysis

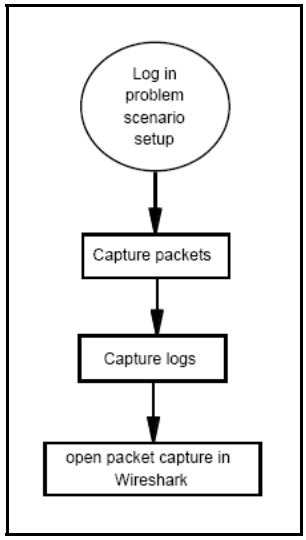
Using the above tree, you start the analysis using the following steps:

1. Do all clients have this problem? If so, check the SPS endpoint configuration.
2. If only a few clients have this problem, set up the scenario with one client as described in "Log in problem scenario setup" (page 32) to capture the information.
3. Analyze the information captured, as described in "Client log in problem analysis" (page 34).

Log in problem scenario setup

This procedure captures the information required for analysis of the problem.

Figure 2
Log in problem scenario setup tree



Procedure steps

Step	Action
1	Configure a client to use HTTP instead of HTTPS. Using HTTP means the packets are not encrypted, and removes the use of certificates.
2	Reproduce the problem.
3	If the problem does not reproduce, you need to check the certificates.
4	If the problem reproduces, start the packet capture.
5	Reproduce the problem.
6	Stop the packet capture.

Attention: Keep the packet traces as small as possible, especially in a busy system.

7	Capture the logs. You capture the logs now so that you have complete information, in case you need to involve Avaya.

8 Open the packet capture in Wireshark.

9 In the filter field, enter **HTTP || SIP**

Attention: In the filter, || means logical or. The | character on most PC keyboards is Shift+\

--End--

Client log in problem analysis

Use this process to analyze the data captured.

Figure 3
Client log in problem analysis (part 1)

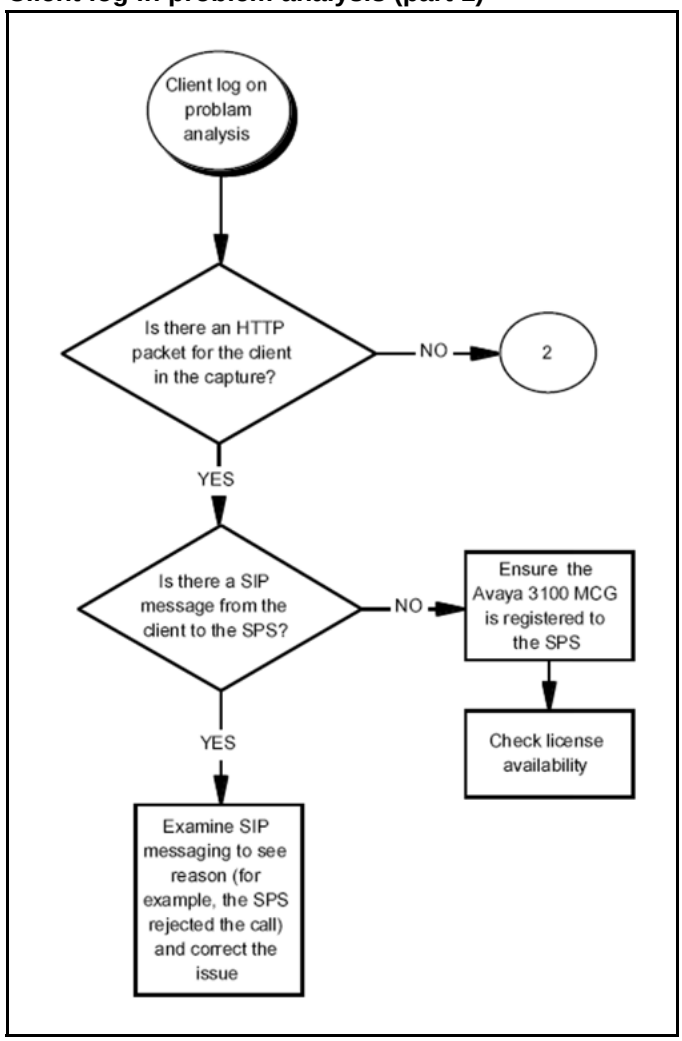
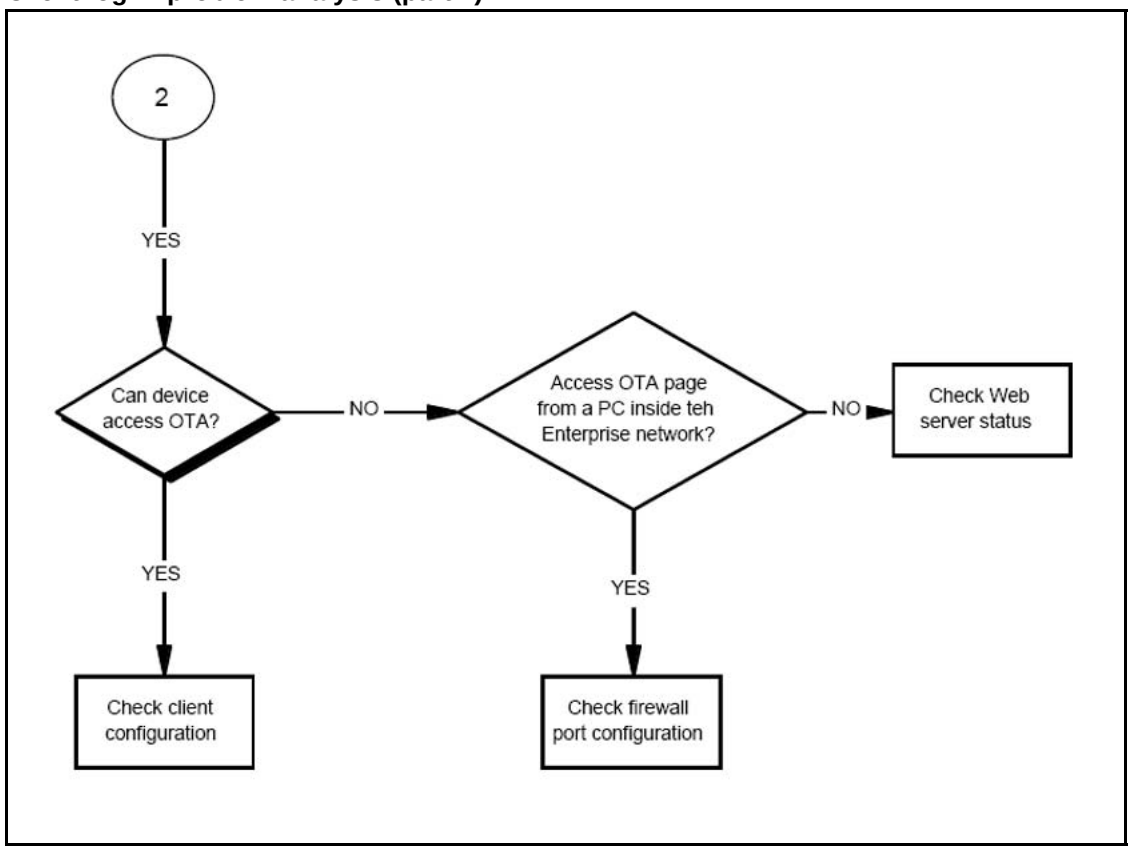

Client log on problam analysis
Is there an HTTP packet for the client in the capture?
NO
2
YES
Is there a SIP message from the client to the SPS?
NO
Ensure the Avaya 3100 MCG is registered to the SPS
Check license availability
YES
Examine SIP messaging to see reason (for example, the SPS rejected the call) and correct the issue

Figure 4
Client log in problem analysis (part 2)



Prerequisites

- "Log in problem scenario setup" (page 32)

Procedure steps

Step	Action
1	In the packet capture, look for the HTTP POST request. You can see the user name and other details in the XML body of the message.
2	If the HTTP packet for the client does not exist, go to step 6.
3	In the packet capture, using the URL fields of the HTTP POST, look for the `SIP` response for the log in attempt to the SPS.
4	If the log in succeeded, the `SIP` message contains the reason that the log in is rejected. Correct the associated issue.

5 If the log in failed,

- Check that the Avaya 3100 Mobile Communicator Gateway is registered to the SPS.
- Check the availability of licences on the Avaya 3100 Mobile Communicator Gateway.

6 Attempt to access the Over the Air (OTA) download site from the device browser.

7 If the OTA page is accessible, then it is likely that the client is not configured correctly. Check the client configuration parameters.

8 If the OTA page is not accessible, attempt to access the OTA page from a PC inside the Enterprise network.

9 If the OTA page is accessible, check the firewall port configuration.

10 If the OTA page is not accessible, check the Avaya 3100 Mobile Communicator Gateway web server status and restart the processes if necessary.

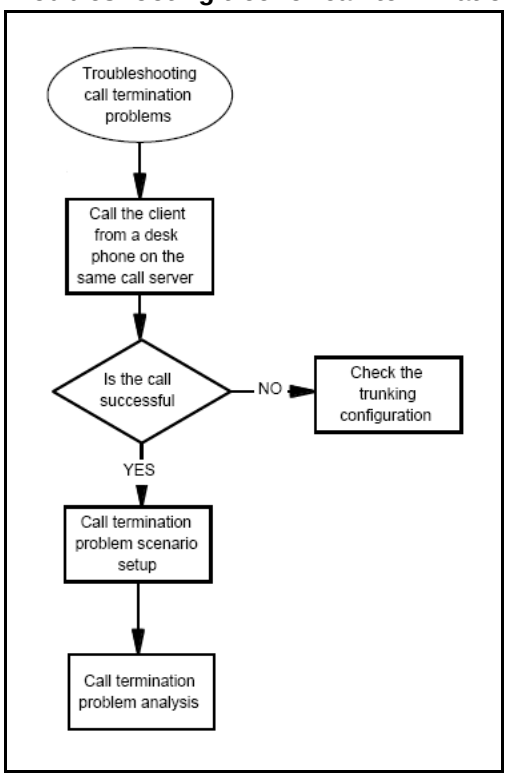
--End--

Troubleshooting call termination problems

Use this section to troubleshoot problems with call termination.

Figure 5 " Troubleshooting tree for call termination problem" (page 37) shows the troubleshooting tree for this problem.

Figure 5
Troubleshooting tree for call termination problem


Troubleshooting call termination problems
Call the client from a desk phone on the same call server
Is the call successful
NO
Check the trunking configuration
YES
Call termination problem scenario setup
Call termination problem analysis

Using the above tree, you start the analysis using the following steps:

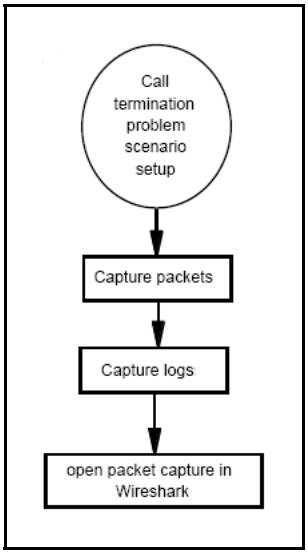
1. Using a desk telephone that is configured on the same call server as the UEXT of the client, make a call to the client.
2. If the call can be made, check the trunking configuration.

3. If the call cannot be made, set up the scenario with one client as described in "Call termination problem scenario setup" (page 38) to capture the information.
4. Analyze the information captured, as described in "Call termination problem analysis" (page 40).

Call termination problem scenario setup

This procedure captures the information required for analysis of the problem.

Figure 6
Call termination scenario setup tree



Procedure steps

Step	Action
1	Configure a client to use HTTP instead of HTTPS. Using HTTP means the packets are not encrypted, and removes the use of certificates.
2	Reproduce the problem.
3	If the problem does not reproduce, you need to check the certificates.
4	If the problem reproduces, start the packet capture.
5	Reproduce the problem.
6	Stop the packet capture.

Attention: Keep the packet traces as small as possible, especially in a busy system.

7 Capture the logs.

You capture the logs now so that you have complete information, in case you need to involve Avaya.

8 Open the packet capture in Wireshark.

9 In the filter field, enter **HTTP || SIP**

Attention: In the filter, || means logical or. The | character on most PC keyboards is Shift+\

--End--

Call termination problem analysis

Use this process to analyze the data captured.

Figure 7
Call termination problem analysis (part 1)

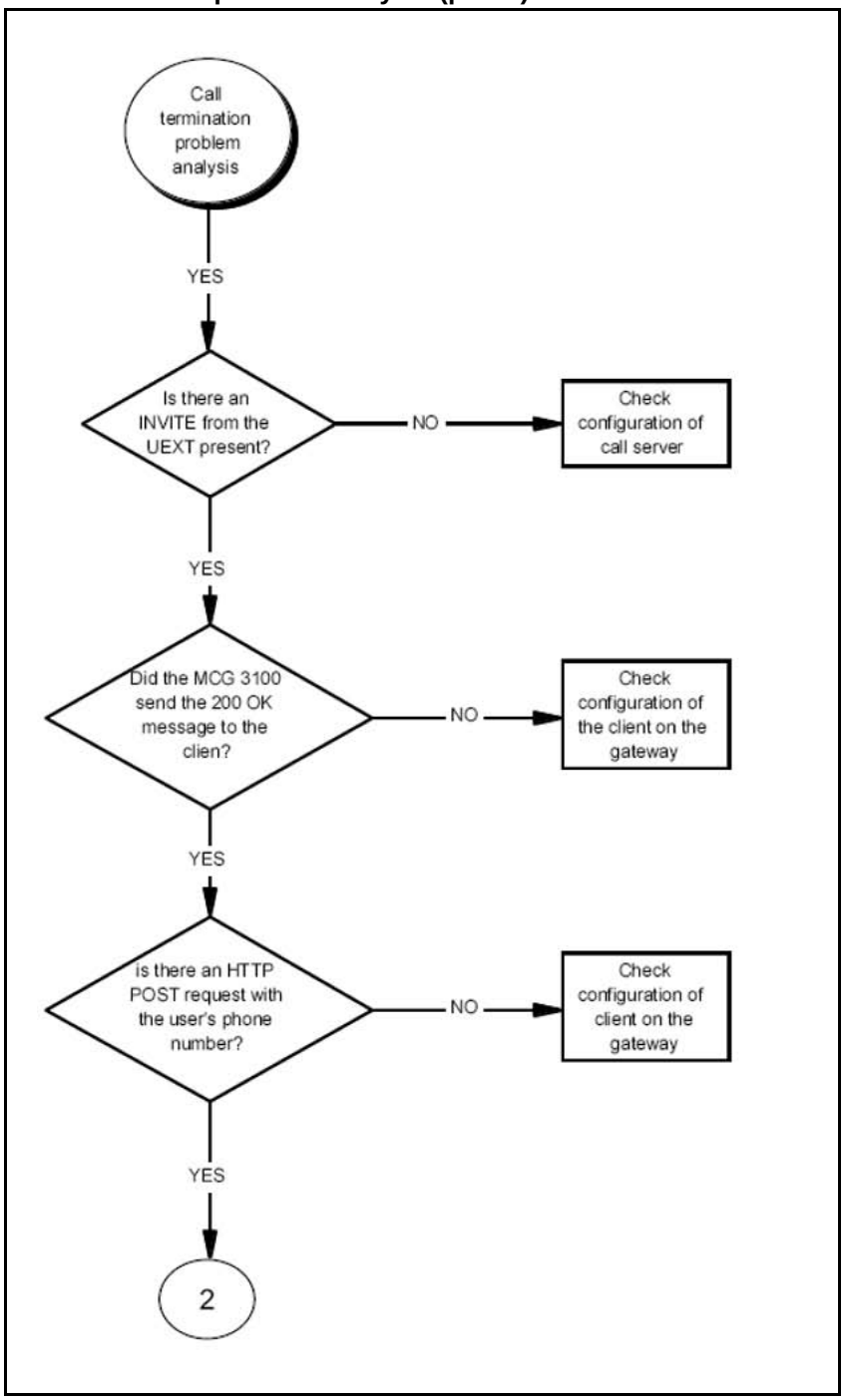
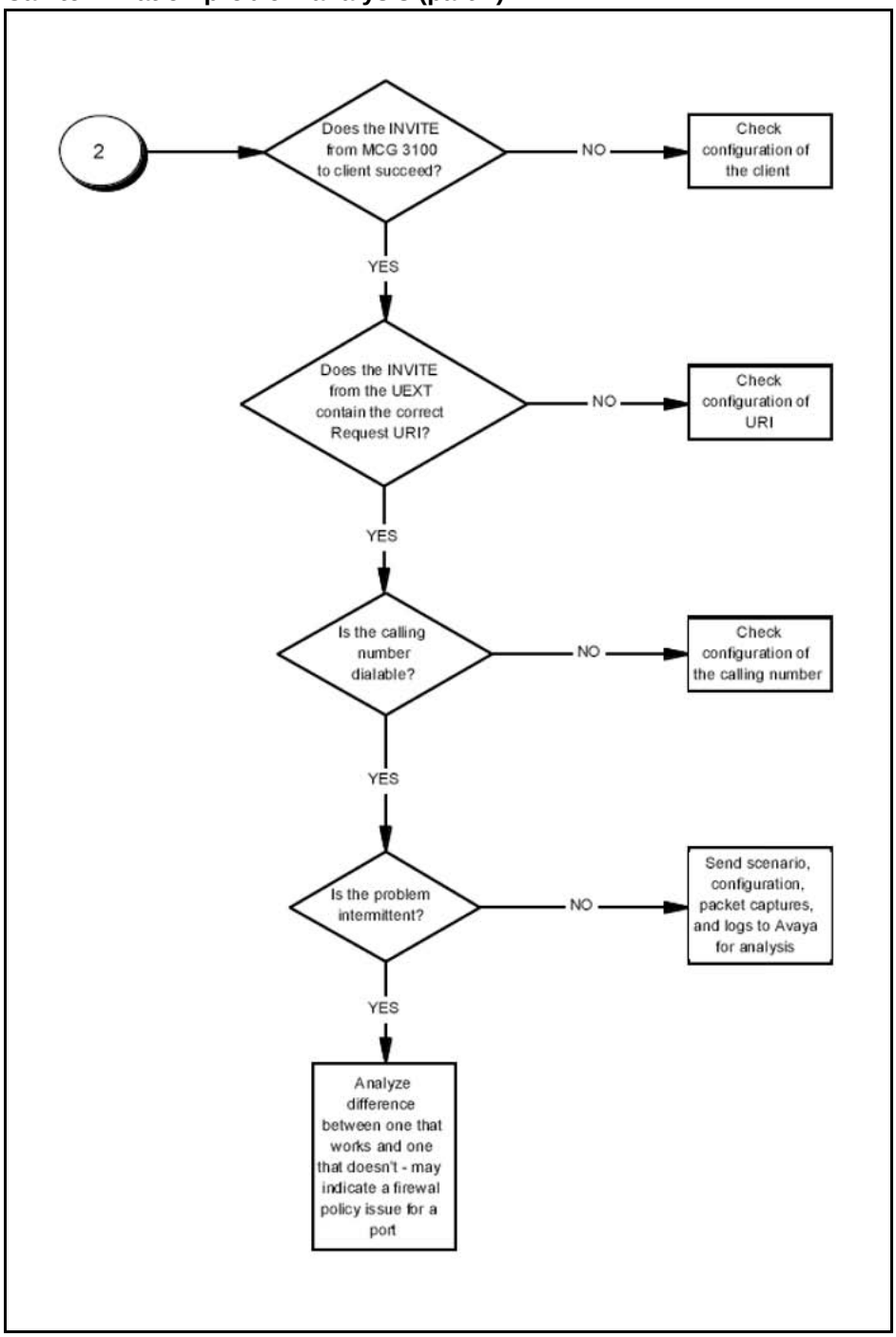

Call termination problem analysis
YES
Is there an INVITE from the UEXT present?
NO
Check configuration of call server
YES
Did the MCG 3100 send the 200 OK message to the clien?
NO
Check configuration of the client on the gateway
YES
is there an HTTP POST request with the user's phone number?
NO
Check configuration of client on the gateway
YES
2

Figure 8
Call termination problem analysis (part 2)


2
Does the INVITE from MCG 3100 to client succeed?
NO
Check configuration of the client
YES
Does the INVITE from the UEXT contain the correct Request URI?
NO
Check configuration of URI
YES
Is the calling number dialable?
NO
Check configuration of the calling number
YES
Is the problem intermittent?
NO
Send scenario, configuration, packet captures, and logs to Avaya for analysis
YES
Analyze difference between one that works and one that doesn't - may indicate a firewal policy issue for a port

Prerequisites

- "Call termination problem scenario setup" (page 38)

Procedure steps

Step	Action
1	In the packet capture, look for the `INVITE` message from the UEXT.
2	If the `INVITE` message is not present, check the configuration of the device on the call server.
3	Look for the `180 ringing` message from the call server to the gateway and determine if the gateway sends the `200 OK` message to the client.
4	If the `200 OK` message does not appear, check the configuration of the client on the gateway.
5	Look for an HTTP POST request with the user's phone number that the Avaya 3100 Mobile Communicator - Client user requested to answer the call.
6	If an HTTP POST request is not available with the user's phone number, check the configuration of the client on the gateway.
7	In the packet capture, look for the `INVITE` message from the Avaya 3100 Mobile Communicator Gateway to the answer destination.
8	If the `INVITE` message is not present, check the configuration of the client.
9	In the packet capture, look for the `INVITE` message from the UEXT contains the correct Request URI.
10	If the `INVITE` message from the UEXT does not contain the correct Request URI, check the configuration of the URI.
11	Look for a valid dialable number that the user is trying to answer.
12	If the calling number is not valid, check the configuration of the calling number.
13	If the problem is intermittent, look for the difference between a trace that works and one that does not. It may indicate a Firewall policy issue for a port.
14	If the problem is not intermittent, send the scenario, configuration, packet captures, and logs to Avaya for analysis.

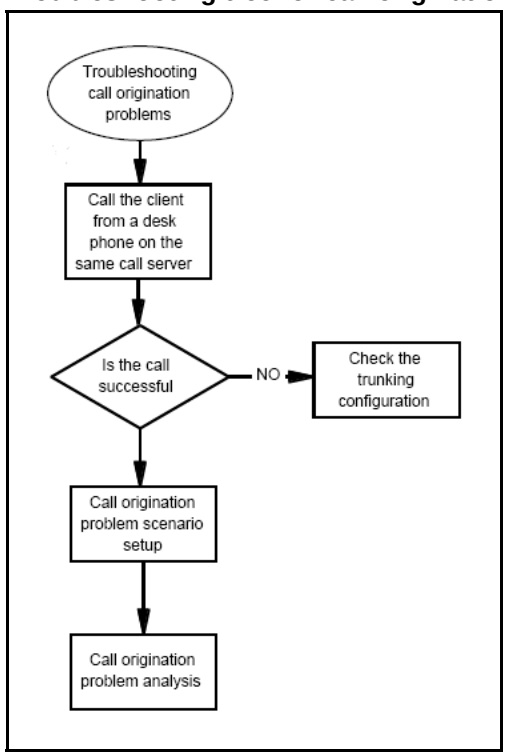
--End--

Troubleshooting call origination problems

Use this section to troubleshoot problems with call origination.

Figure 9 " Troubleshooting tree for call origination problems" (page 43) shows the troubleshooting tree for this problem.

Figure 9
Troubleshooting tree for call origination problems


Troubleshooting call origination problems
Call the client from a desk phone on the same call server
Is the call successful
NO
Check the trunking configuration
Call origination problem scenario setup
Call origination problem analysis

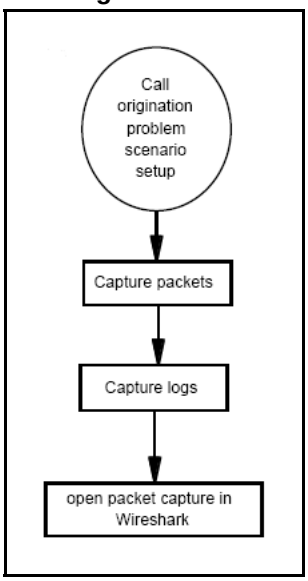
Using the above tree, you start the analysis using the following steps:

1. Do all clients share the call origination problem? If so, check the trunking configuration.
2. If only a few clients have problems with call origination, set up the scenario with one client as described in "Call origination problem scenario setup" (page 44) to capture the information.
3. Analyze the information captured, as described in "Call origination problem analysis" (page 46).

Call origination problem scenario setup

This procedure captures the information required for analysis of the problem.

Figure 10
Call origination scenario setup tree



Procedure steps

Step	Action
1	Configure a client to use HTTP instead of HTTPS. Using HTTP means the packets are not encrypted, and removes the use of certificates.
2	Reproduce the problem.
3	If the problem does not reproduce, you need to check the certificates.
4	If the problem reproduces, start the packet capture.
5	Reproduce the problem.
6	Stop the packet capture.

Attention: Keep the packet traces as small as possible, especially in a busy system.

7 Capture the logs.

You capture the logs now so that you have complete information, in case you need to involve Avaya.

8 Open the packet capture in Wireshark.

9 In the filter field, enter **HTTP || SIP**

Attention: In the filter, || means logical or. The | character on most PC keyboards is Shift+\

--End--

Call origination problem analysis

Use this process to analyze the data captured.

Figure 11
Call origination problem analysis (part 1)

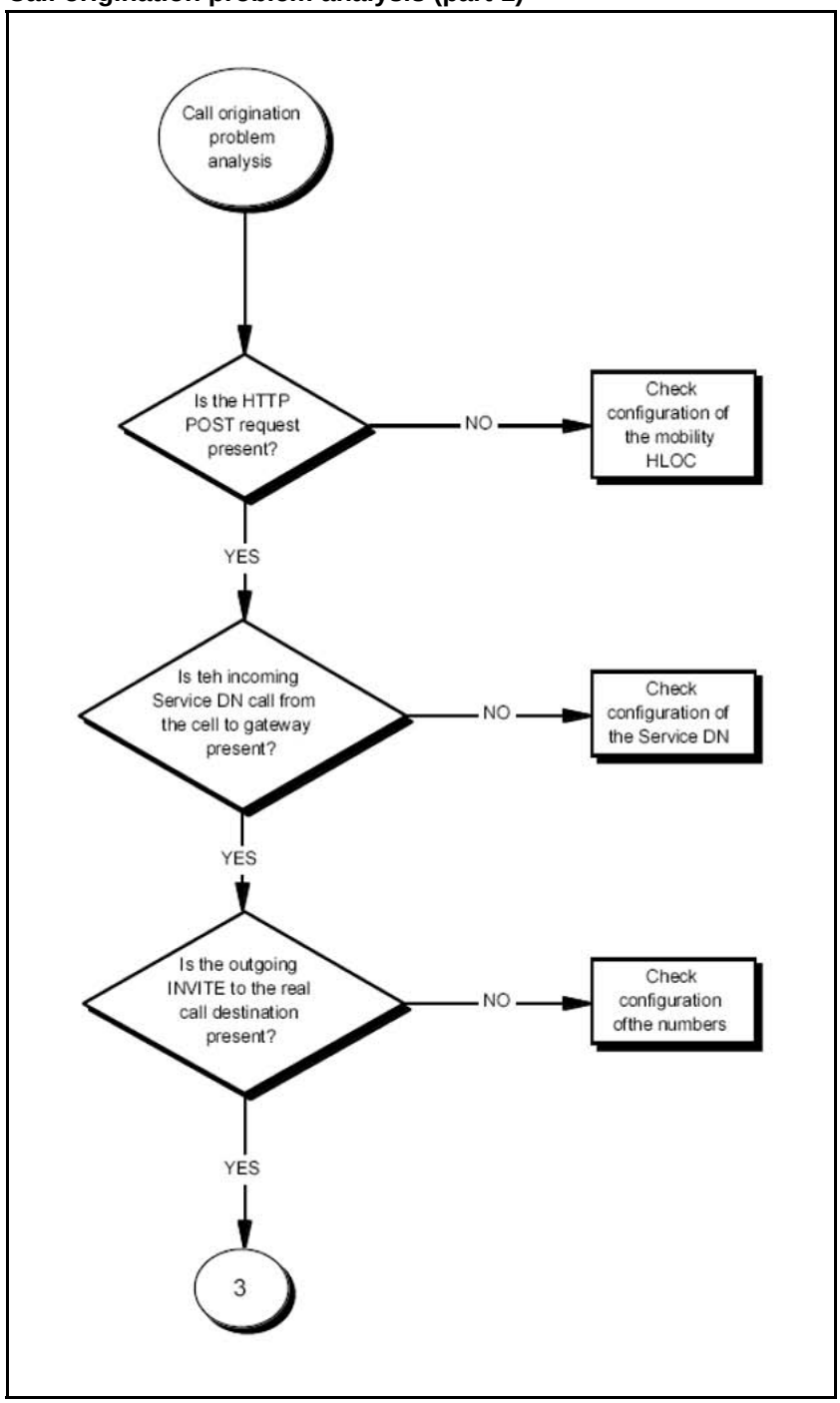


Figure 12
Call origination problem analysis (part 2)

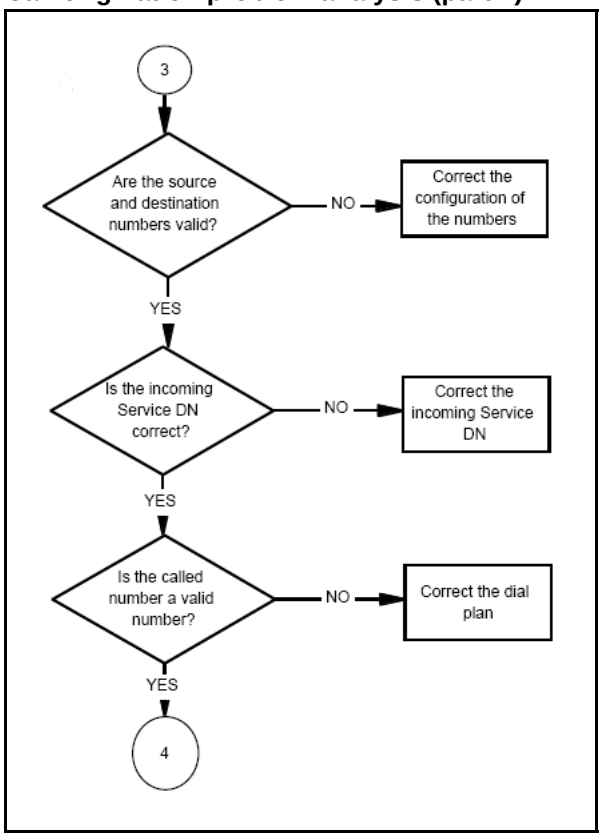
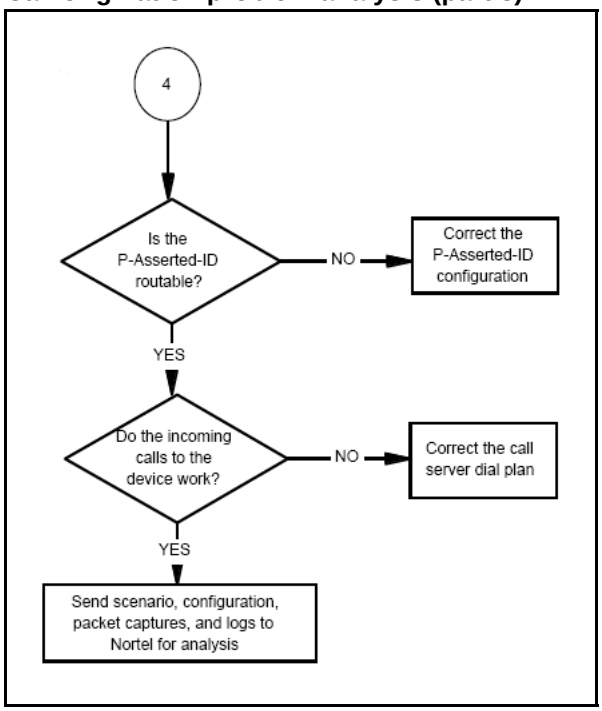


Figure 13
Call origination problem analysis (part 3)



Prerequisites

- "Call origination problem scenario setup" (page 44)

Procedure steps

Step	Action
1	In the packet capture, look for the HTTP POST request from the client that contains the call attempt request.
2	If the HTTP POST request is not present, check the configuration of the mobility HLOC.
3	Look for the incoming service DN call from the cell phone to the Avaya 3100 Mobile Communicator Gateway.
4	If the incoming service DN call is not present, check configuration of the service DN.
5	In the packet capture, look for the outgoing `INVITE` message to the real call destination.
6	If the outgoing `INVITE` message is not present, check the configuration of the call destination.
7	In the packet capture, look for valid source and destination numbers.

8	If the source and destination numbers are not valid, correct the configuration of the numbers.
9	In the packet capture, look for a valid incoming service DN call.
10	If the incoming Service DN call is not valid, correct the incoming Service DN.
11	Look for valid called number in the current dial plan.
12	If the called number is not a valid number, correct the dial plan.
13	In the packet capture, look for the P-Asserted-ID message for the call attempt from the Avaya 3100 Mobile Communicator Gateway.
14	If the P-Asserted-ID is not routable, correct the P-Asserted-ID configuration.
15	Try making a call to the device directly.
16	If you can call the device directly, send the scenario, configuration, packet captures, and logs to Avaya for analysis.
17	If the incoming calls to the device does not work, correct the call server dial plan.

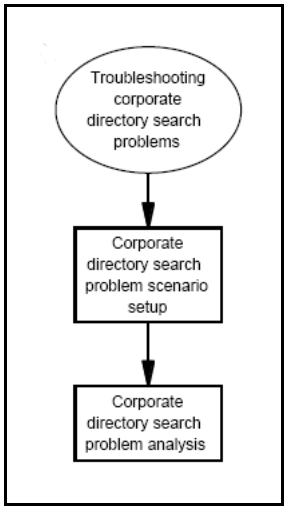
--End--

Troubleshooting corporate directory search problems

Use this section to troubleshoot problems with corporate directory search.

Figure 14 " Troubleshooting tree for corporate directory search problems" (page 51) shows the troubleshooting tree for this problem.

Figure 14
Troubleshooting tree for corporate directory search problems


Troubleshooting corporate directory search problems
Corporate directory search problem scenario setup
Corporate directory search problem analysis

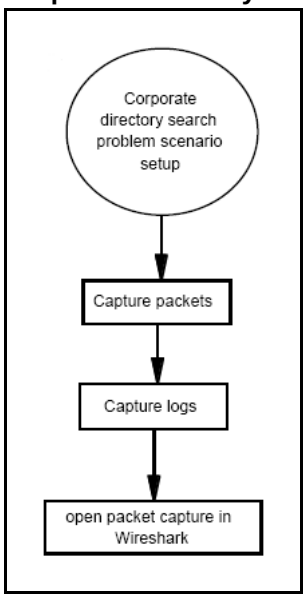
Using the above tree, you start the analysis using the following steps:

1. Do all clients have problem with the corporate directory search? If so, set up the scenario with one client as described in "Corporate directory search problem scenario setup" (page 52) to capture the information.
2. Analyze the information captured, as described in "Corporate directory search problem analysis" (page 54).

Corporate directory search problem scenario setup

This procedure captures the information required for analysis of the problem.

Figure 15
Corporate Directory search scenario setup tree



Procedure steps

Step	Action
1	Configure a client to use HTTP instead of HTTPS. Using HTTP means the packets are not encrypted, and removes the use of certificates.
2	Reproduce the problem.
3	If the problem does not reproduce, you need to check the certificates.
4	If the problem reproduces, start the packet capture.
5	Reproduce the problem.
6	Stop the packet capture. **Attention:** Keep the packet traces as small as possible, especially in a busy system.
7	Capture the logs.

You capture the logs now so that you have complete information, in case you need to involve Avaya.

8 Open the packet capture in Wireshark.

9 In the filter field, enter **HTTP || SIP**

Attention: In the filter, || means logical or. The | character on most PC keyboards is Shift+\

--End--

Corporate directory search problem analysis

Use this process to analyze the data captured.

Figure 16
Corporate directory search problem analysis (part 1)

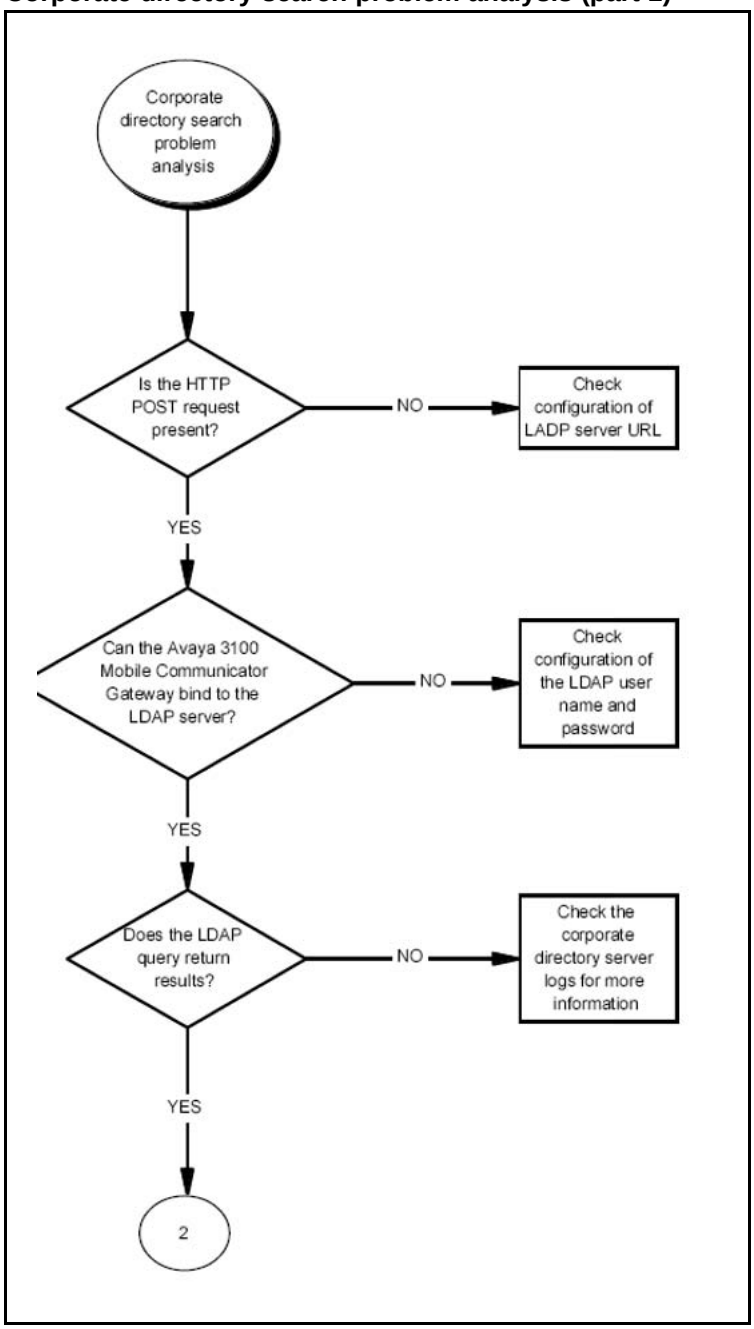
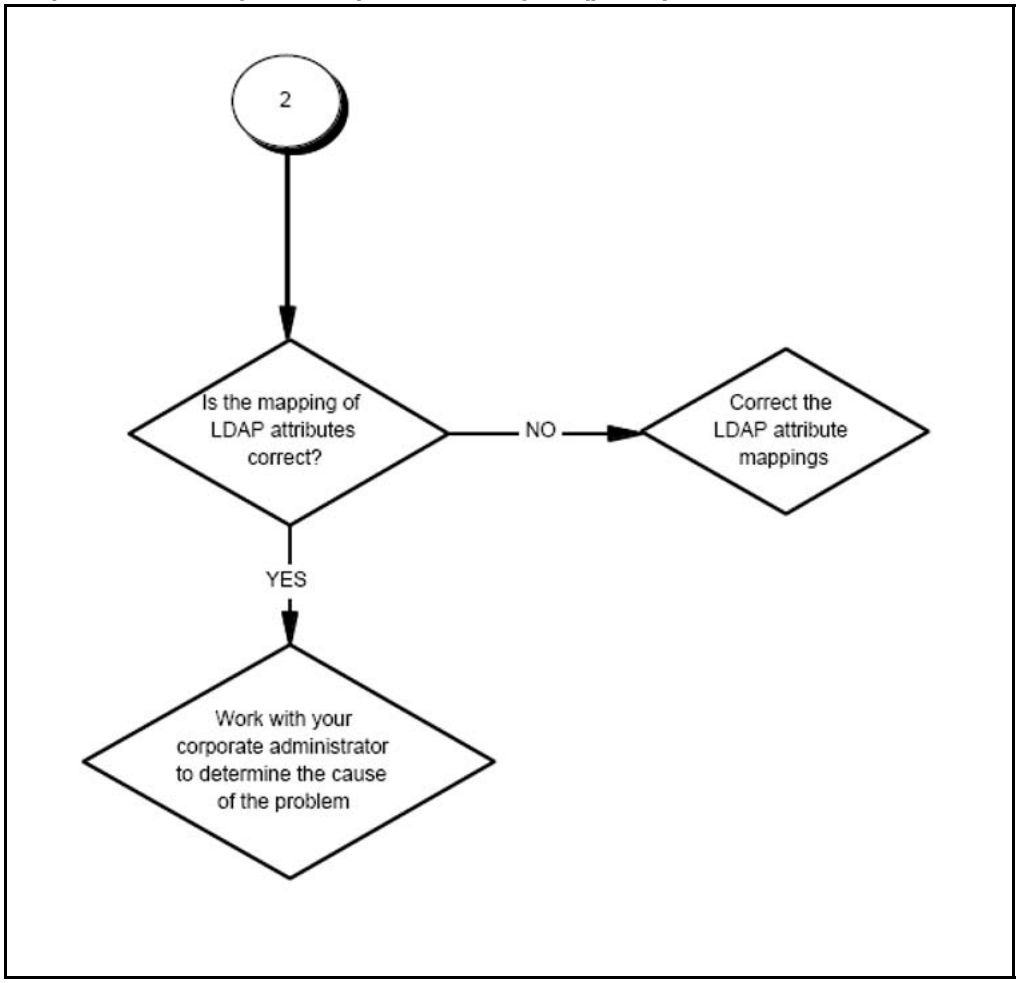

Corporate directory search problem analysis
Is the HTTP POST request present?
NO
Check configuration of LADP server URL
YES
Can the Avaya 3100 Mobile Communicator Gateway bind to the LDAP server?
NO
Check configuration of the LDAP user name and password
YES
Does the LDAP query return results?
NO
Check the corporate directory server logs for more information
YES
2

Figure 17
Corporate directory search problem analysis (part 2)


2
Is the mapping of LDAP attributes correct?
NO
Correct the LDAP attribute mappings
YES
Work with your corporate administrator to determine the cause of the problem

Procedure steps

Step	Action
1	In the packet capture, look for the HTTP POST request from the client that contains the directory search request.
2	If the HTTP POST request is not present, check the configuration of LDAP server URL.
3	Check for the Avaya 3100 Mobile Communicator Gateway bind with the LDAP server.
4	If the Avaya 3100 Mobile Communicator Gateway does not bind with the LDAP server, check the configuration of LDAP username and password.
5	In the packet capture, look for the LDAP query request results.

6 If the LDAP query request does not return results, check the corporate directory server logs for more information.

7 Look for the mapping of the phone numbers to LDAP attributes on the Avaya 3100 Mobile Communicator Gateway.

8 If the mapping of the phone numbers to LDAP attributes is correct, work with your corporate directory administrator to determine the cause of the problem.

9 If the mapping of the phone numbers to LDAP attributes is not correct on the Avaya 3100 Mobile Communicator Gateway, check the LDAP attribute mappings.

--End--